UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI

ALYSSA KRUTSINGER, individually and on behalf of all others similarly situated, Plaintiff, v. POWERSCHOOL HOLDINGS, INC. and POWERSCHOOL GROUP LLC, Defendants.	Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Alyssa Krutsinger ("Krutsinger" or "Plaintiff"), by and through the undersigned counsel, brings this class action complaint against Defendants PowerSchool Holdings, Inc. and PowerSchool Group LLC (collectively, "PowerSchool" or "Defendants"), individually and on behalf of all others similarly situated ("class members"). Plaintiff makes the following allegations based upon personal knowledge as to her own actions, and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE CASE

1. Plaintiff brings this class action on behalf of herself, and all others similarly situated against PowerSchool for its failure to secure and safeguard the student educational records, and personally identifiable information of millions of its users, including students, teachers, and their families.

2. PowerSchool touts itself as "a leading provider of cloud-based software in K-12

education in North America."[1] The company's software as a service platform provides services for multiple aspects of education, including student information systems, learning management and analytics.[2] "PowerSchool supports over 60 million students and over 18,000 customers [who are educational institutions] in more than 90 countries, including more than 90 of the top 100 [school] districts by student enrollment in the United States."[3] PowerSchool's wide deployment and usage put many of its customers, educators and family communities at risk.

3. One product, central to PowerSchool's offerings, is its PowerSchool Student Information System ("SIS"). PowerSchool markets this software product as a "secure customizable platform providing the interoperability need to power your school and district operations with accurate student data."[4] Notably, the PowerSchool SIS product is not limited to gathering and maintaining student data alone; it also allows for "gather[ing] vital information from families and staff."[5]

4. As evidenced by PowerSchool's repeated public representations, PowerSchool understood the highly sensitive nature of the personal information it was gathering and maintaining in its regular course of business. This highly sensitive information includes names, email addresses, phone numbers, Social Security numbers, medical information, dates of birth, and other related information (collectively "Private Information").[6]

5. On January 7, 2025, PowerSchool notified its customers of a cybersecurity incident

---

[1] https://www.powerschool.com/company/
[2] https://www.techtarget.com/whatis/feature/PowerSchool-data-breach-Explaining-how-it-happened
[3] https://www.powerschool.com/bain-capital/#:~:text=About%20PowerSchool&text=PowerSchool%20supports%20over%2060%20million,at%20www.powerschool.com
[4] https://www.powerschool.com/student-informationcloud/powerschool-sis/#video
[5] *Id.*
[6] https://www.powerschool.com/security/sis-incident-2/

(the "Data Breach") that exposed the personal data of students, teachers, and their families. PowerSchool admitted it discovered the breach on December 28, 2024, which involved unauthorized access and exfiltration of Private Information from specific PowerSchool SIS environments via its PowerSource customer support portal.[7]

6. The hackers responsible for the breach claimed that they stole the personal information of 62.4 million students and 9.5 million teachers.[8] PowerSchool reportedly paid a ransom hoping to prevent the public release of the stolen data,[9] which dates back to 2005.[10]

7. As a direct and proximate result of PowerSchool's failure to protect the sensitive information it was entrusted to safeguard, Plaintiff and class members have already suffered harm and have been exposed to a significant and continuing risk of identity theft, financial fraud, and other identity-related fraud from now and into the indefinite future.

PARTIES

8. Plaintiff Alyssa Krutsinger is a resident of North Kansas City, Missouri and former student of the Liberty School District in Missouri who provided her Private Information to PowerSchool.

9. Defendant PowerSchool Holdings, Inc. is a Delaware corporation with its principal place of business at 150 Parkshore Dr., Folsom, California 95630.

10. Defendant PowerSchool Group LLC is a Delaware corporation with its principal place of business at 150 Parkshore Dr., Folsom, California 95630. PowerSchool Group LLC is a

---

[7] https://www.powerschool.com/security/sis-incident-2/
[8] https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/
[9] https://www.infosecurity-magazine.com/news/powerschool-pays-ransom-data-leak/
[10] https://www.yorkregion.com/news/york-board-says-powerschool-data-breach-includes-student-staff-information-dating-back-to-2005/article_4e828dad-c983-56b3-abf3-8054859072aa.html

wholly owned subsidiary of PowerSchool Holdings, Inc., and is registered to do business in the State of Missouri and can be served through its Missouri Registered Agent, United Corporate Services, Inc. located at 915 Southwest Blvd., Suite N, Jefferson City, MO 65109.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d) because: (i) there are more than 100 class members; (ii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs; and (iii) there is minimal diversity because at least one class members is a citizen of a state different from that of Defendant.

12. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant conducts much of their business in this District and Defendant has caused harm to class members residing in this District.

FACTUAL ALLEGATIONS

PowerSchool's Privacy Practices

13. PowerSchool, founded in 1997, holds itself out to the public as "a leading provider of cloud-based software in North America" with a vision "to transform education using innovative technology that truly supports personalized education for all students around the world."[11]

14. As a condition of using its education technology software and services, PowerSchool requires that its users, including Plaintiff and class members, entrust it with their sensitive information, including their names, contact information, dates of birth, limited medical alert information, Social Security Numbers, and other related information.[12]

[11] https://www.powerschool.com/company/
[12] https://www.powerschool.com/security/sis-incident-2/

15. Given the amount and sensitive nature of the data it collects, PowerSchool maintains a "Global Privacy Statement" and uses "Privacy Principles" as a guide to inform its approach to data privacy and data protection.[13] PowerSchool represents, among other things, that PowerSchool does not sell or share its customers' and users' data to third parties without consent.[14]

16. PowerSchool understands the importance of protecting customers' and users' educational records and Private Information and commits "to being a good custodian of student data – taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability."[15]

17. PowerSchool recognizes that safeguarding the privacy of its users is a matter of highest importance and assures its customers and users that it "employs a variety of physical, administrative, and technological safeguards designed to protect your data against loss, misuse, and unauthorized access or disclosure" and that it stives "to continuously maintain reasonable physical, administrative, and technical security measures."[16]

18. PowerSchool further assures its customers and users that its "systems are regularly certified by third parties against industry security standards from AIPCA and ISO," and that it "independently verifies its security management system to the internationally recognized standard for security management and holds ISO 27001 and SOC2 certifications."[17]

19. Despite acknowledging its duty and publicly representing its commitment to security, PowerSchool failed to implement reasonable safeguards or policies to protect Plaintiff's and class members' Private Information.

---

[13] https://www.powerschool.com/privacy/
[14] *Id.*
[15] https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/
[16] https://www.powerschool.com/privacy/
[17] *Id.*

The Data Breach

20. On January 7, 2025, PowerSchool sent its customers a Notice of Data Breach (the "Notice").[18] The Notice provided the following information:

> [W]e are reaching out to inform you that on December 28, 2024, PowerSchool become aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals, PowerSource. Over the succeeding days, our investigation determined that an unauthorized party gained access to certain PowerSchool Student Information System ("SIS") customer data using a compromised credential, and we regret to inform you that your data was accessed.
>
> * * *
>
> As soon as we learned of the potential incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. We have also informed law enforcement.
>
> We can confirm that the information accessed belongs to certain SIS customers and relates to families and educators, including those from your organization.[19]

21. On or about January 24, 2025, PowerSchool updated its website regarding the SIS incident, admitting that the "types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Security Number (SSN), and other related information."[20]

22. According to *BleepingComputer*, the hackers responsible for the PowerSchool breach claimed to have stolen data from 6,505 school districts across the United States, Canada, and other countries as part of an extortion demand made to the company.[21]

23. *BleepingComputer* reported that the PowerSchool data breach allegedly impacted

---

[18] https://www.powerschool.com/security/sis-incident-2/
[19] https://www.local3news.com/local-news/walker-co-schools-alerting-parents-educators-of-student-information-system-data-breach/article_1505632e-cd40-11ef-9e46-e7788d8f6b28.html
[20] https://www.powerschool.com/security/sis-incident-2/
[21] https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/

62,488,628 students and 9,506,624 teachers. [22]

24. PowerSchool has not disclosed the full extent of the Data Breach's impact on its systems. Instead, it instructs users to "reach out to your school directly" to determine if their or their children's Private Information was affected. PowerSchool has not clarified how many of the 60 million student records it holds were impacted or provided a timeline for notifying Plaintiff and class members.[23]

25. According to the Notice, "an unauthorized party gained access" to PowerSchool's system through the use of "a compromised credential." Compromised credentials account for nearly two-thirds of all data breaches.[24] This occurs when unauthorized users obtain valid login information for authorized accounts. Common causes include reusing passwords across multiple websites, failing to update passwords regularly, or relying on overly simplistic passwords.

26. Entities and individuals can protect themselves from the use of compromised credentials through the use of multi-factor authentication (MFA), which provides an additional layer of security by requiring more than just a username and password to verify a user's identity.

27. The use of MFA is MFA is widely recognized as a critical component of digital security. While passwords can be easily obtained on the black market, MFA adds a layer of protection that can secure accounts even if credentials are compromised. Both the National Institute of Standards and Technology ("NIST") [25] and private sector companies like Microsoft recommend MFA due to its proven effectiveness in enhancing system security.[26]

---

[22] *Id*.
[23] *Id.*
[24] https://www.zengrc.com/blog/compromised-credentials-could-put-your-business-at-risk/
[25] https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication
[26] https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437- 121c-be60-d123-eda06bddf661

28. PowerSchool failed to implement MFA to secure its systems or relied on improperly configured MFA, despite its use being widely recognized as a best practice for digital security.[27]

29. PowerSchool claims that it is "committed to being a good custodian of student data, taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability," yet it failed to require industry-standard data security safeguards. Had PowerSchool implemented these commonsense security measures, cybercriminals never could have accessed millions of individuals' data, and the Data Breach would have been prevented or much smaller in scope.

The Data Breach Was Preventable

30. Educational institutions and their associated vendors are acutely aware that their databases are a central target of cybercriminals due to their storage of vast amounts of Private Information, including confidential student records. Data breaches of education-related organizations are occurring with increased frequency because educational institutions collect sensitive Private Information.[28]

31. According to *Education Week*, "55 percent of K-12 school data breaches between 2016 and 2021 were carried out on ed-tech vendors," [29] and "Research from Comparitech shows that data breaches have affected more than 37.6 million records across K-12 schools and higher education since 2005. Between 2018 and 2021, 61% of targeted institutions in the United States

[27] https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/
[28] https://www.npr.org/2024/03/11/1236995412/cybersecurity-hackers-schools-ransomware.
[29] https://www.edweek.org/technology/ed-tech-companies-are-vulnerable-to-cyberattacks-a-new-federal-effort-wants-to-help/2024/05

education sector were K-12 schools."[30]

32. According to *EdTech Focus on Higher Education*, cyberattacks in higher education increased by 70% between 2022 and 2023. The report notes that these figures only account for incidents where a ransom was not paid, suggesting the actual number of attacks is likely much higher.[31]

33. PowerSchool was fully aware of its obligation to protect its customers' and users' Private Information, and the risks associated with failing to do so. PowerSchool observed frequent public announcement of data breaches affecting education and edtech industries and knew that the information of the type collected, maintained, and stored by PowerSchool is highly coveted and a frequent target of hackers.

34. For example, "in early 2022, ed-tech firm Illuminate Education suffered a data breach; free lunch, special education and other data for more than 800,000 current and former New York public school students was compromised."[32]

35. Additionally, in January 2024, Raptor Technologies, a school safety software company, experienced a data breach that exposed around 4 million records. "The cybersecurity leak—which the company says is now patched—included thousands of documents detailing emergency plans at U.S. schools, including lockdown procedures."[33]

36. In 2018, "a data breach at K12 Inc., a leading provider of online education, exposed the personal information of over 1 million students. In 2020, a data breach at Pearson, another

---

[30] https://www.darkreading.com/vulnerabilities-threats/education-industry-data-must-be-protected
[31] https://edtechmagazine.com/higher/article/2024/03/cyberattacks-higher-ed-rose-dramatically-last-year-report-shows
[32] https://www.govtech.com/cdg/what-does-the-ed-tech-explosion-mean-for-student-privacy
[33] https://www.edweek.org/technology/a-massive-data-leak-exposed-school-lockdown-plans-what-districts-need-to-know/2024/01

major EdTech company, exposed the personal information of over 50 million students."[34]

37. Student records are particularly valuable to identity thieves and other criminals, because such records provide a complete profile of an individual and that individual is more likely to have no previous credit history, making their Private Information particularly useful for financial scams.

38. The Department of Education has identified the value of a student record on the black market at $250-$300, a fact known to PowerSchool, as it uses this figure to promote its own products.[35]

39. At all times relevant, PowerSchool knew, or reasonably should have known, of the importance of safeguarding Private Information and the foreseeable consequences that would occur if it failed to do so, including, specifically, the significant costs that would be imposed on affected individuals as a result of the breach.

40. Despite the publicly available knowledge of the serious threat of compromises of Private Information, and despite collecting, storing and maintaining the Private Information of millions of individuals, PowerSchool failed to use reasonable care in maintaining and overseeing the privacy and security of Plaintiff's and class members' Private Information.

Allegations Relating to Plaintiff

41. Plaintiff Alyssa Krutsinger is and at all relevant times was a citizen of the State of Missouri and the United States.

42. Plaintiff Krutsinger was a PowerSchool user prior to the time of the data breach.

43. In the course of receiving education from her school district, Plaintiff Krutsinger

[34] https://www.superchargerventures.com/articles/data-security-in-edtech-the-growing-threat
[35] https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/.

was required, directly or indirectly, to provide her Private Information to PowerSchool. When providing and entrusting PowerSchool with her Private Information, Plaintiff Krutsinger reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

44. Upon information and belief, at the time of the Data Breach, PowerSchool retained Plaintiff's Private Information in its systems.

45. As a result of the Data Breach, Plaintiff Krutsinger has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Krutsinger has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

46. After the Data Breach, Plaintiff Krutsinger has seen an increase in spam texts, emails, and phone calls.

47. To date, Plaintiff Krutsinger has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Krutsinger values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

48. Had Plaintiff Krutsinger been informed of PowerSchool's insufficient data security measures to protect her Private Information, she would not have willingly provided her Private Information to PowerSchool. Given the highly sensitive nature of the Private Information stolen,

and its likely subsequent dissemination to unauthorized parties, Plaintiff Krutsinger has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Krutsinger anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

49. Plaintiff Krutsinger suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) damages for the unauthorized disclosure of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) lifetime cost of credit monitoring, as ongoing protection is necessary to mitigate the heightened risk of identity theft and financial fraud resulting from the Data Breach; and (x) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in PowerSchool's possession and is subject to further unauthorized disclosures so long as PowerSchool fails to undertake appropriate and adequate measures to protect the Private Information.

50. The Data Breach has caused Plaintiff Krutsinger to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

51. As a result of the Data Breach, Plaintiff Krutsinger is and will continue to be at increased risk of identity theft and fraud for years to come.

52. Plaintiff Krutsinger has a continuing interest in ensuring that her Private

Information, which, upon information and belief, remains in PowerSchool's possession, is protected and safeguarded from future breaches.

53. Upon information and belief, PowerSchool continues to store and/or share Plaintiff Krutsinger's Private Information on its internal systems. Thus, Plaintiff Krutsinger has a continuing interest in ensuring that her Private Information is safeguarded from future breaches.

PowerSchool failed to Comply with FTC Guidelines

54. Federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[36]

55. The FTC's publication *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[37] Among other things, the guidelines note that businesses should protect the personal customer information that they collect and store; properly dispose of personal information that is no longer needed; encrypt information stored on their computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[38]

---

[36] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
[37] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf
[38] *Id.*

56. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

57. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[39]

58. PowerSchool was fully aware of its obligation to implement and use reasonable measures to protect the Private Information of its customers but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Defendant's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

The Impact of the Data Breach on Victims

59. Plaintiff's and Class members' highly sensitive Private Information is of great value to cybercriminals, who can use the data stolen in the Data Breach to exploit Plaintiff and the Class members and profit off their misfortune and stolen information. The cybercriminals' motives for the Data Breach were purely nefarious and malicious in nature: their one goal was to access

[39] https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement

systems, including PowerSchool's systems, in order to obtain valuable Private Information to sell on underground markets.

60. As a result of the Data Breach, Plaintiff and class members face several types of identity theft and fraud including financial identity theft, medical identity theft, criminal identity theft, synthetic identity theft, and child identity theft. These forms of identity theft can result in credit card fraud, fraud through government documents and benefits, bank fraud, employment fraud, tax fraud, and medical fraud.[40]

61. Further, malicious actors often wait months or years to use the Private Information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen Private Information, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

62. Children are equally (and especially) at risk of identity theft when their highly sensitive Private Information is compromised. Indeed, credit reporting agencies do not routinely check applicants' age or adequate proof of identity—meaning the agencies will not serve as a sufficient defense against the illicit use of children's name, date of birth, or SSN.[41]

63. PowerSchool's deficient Data Breach notices also caused Plaintiff's and class members' harm. The Data Breach notices failed to explain the precise nature of the attack, the identity of the hackers, or the specific data accessed and stolen for each Data Breach victim. PowerSchool's decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk.

---

[40] https://www.mcafee.com/learn/a-guide-to-identity-theftstatistics/
[41] https://securityintelligence.com/the-looming-crisis-of-child-identity-theft/

64. Plaintiff and class members have a direct interest in PowerSchool's promises and duties to protect their Private Information, *i.e.*, that PowerSchool *not increase* their risk of identity theft and fraud. Because PowerSchool failed to live up to its promises and duties in this respect, Plaintiff and class members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by PowerSchool's wrongful conduct. Through this remedy, Plaintiff and class members seek to restore themselves and class members as close to the same position as they would have occupied but for PowerSchool's wrongful conduct, namely its failure to adequately protect Plaintiff's and class members' Private Information.

65. PowerSchool understands the present and continuing increased risk of harm Plaintiff and class members face as a result of its wrongful conduct, which is why PowerSchool has "engaged TransUnion and Experian . . . to offer two years of complimentary identity protection services . . . for all students and educators whose information from your PowerSchool SIS was involved. PowerSchool will also be offering two years of complimentary credit monitoring services . . . for all students and educators who have reached the age of majority whose information was involved."[42] However, any relief PowerSchool purports to provide will not be sufficient in protecting Plaintiff and class members from the imminent risks of potential identity theft or fraud that they will face for years to come.

66. For the reasons as enumerated above, PowerSchool's conduct, which allowed the Data Breach to occur, caused Plaintiff and class members significant injuries and harm.

CLASS ALLEGATIONS

67. Plaintiff seeks relief individually and as a representative of all others who are

[42] https://www.powerschool.com/security/sis-incident-2/

similarly situated. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and/or (c)(4), Plaintiff seeks certification of a nationwide class and a Missouri subclass, defined as follows:

> **Nationwide Class**: All persons in the United Sates whose Private Information was accessed in the Data Breach.
>
> **Missouri Subclass**: All persons residing in Missouri whose Private Information was accessed in the Data Breach.

68. Both the proposed Nationwide Class and Missouri Subclass will collectively referred to as the Class, except where it is necessary to differentiate.

69. Specifically excluded from the Class are PowerSchool; its officers, directors, or employees; any entity in which PowerSchool has a controlling interest; and any affiliate, legal representative, heir, or assign of PowerSchool. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

70. Class Identity: The members of the Class are readily identifiable and ascertainable. PowerSchool and/or its affiliates, among others, possess the information to identify and contact members of the Class.

71. Numerosity: The Class contains millions of individuals and is so numerous that joinder of all of them is impracticable.

72. Typicality: Plaintiff's claims are typical of the claims of the members of the classes because all Class members had their Private Information compromised in the Data Breach.

73. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no interest antagonistic to those of the Class and are aligned with Class members' interests because Plaintiff was subject to the same Data Breach and experienced the same injuries and harms. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including many significant cases involving data breaches.

74. Commonality and Predominance: There are questions of law and fact common to the classes. These common questions predominate over any questions affecting only individual Class members. The common questions of law and fact include, without limitation:

a. Whether PowerSchool violated statutes including the FTC;

b. Whether PowerSchool owed Plaintiff and Class members a duty to implement and maintain reasonable security procedures and practices to protect their Private Information;

c. Whether PowerSchool breached an express or implied contract with Plaintiff and Class members, including whether PowerSchool breached an agreement with Plaintiff and class members to keep their Private Information confidential;

d. Whether PowerSchool acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class members' Private Information;

e. Whether PowerSchool breached its duty to implement reasonable security systems to protect Plaintiff's and Class members' Private Information;

f. Whether PowerSchool's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and Class members;

g. Whether PowerSchool breached its third-party beneficiary contract with Plaintiff and Class members;

h. Whether PowerSchool fixed the vulnerabilities that enabled the Data Breach;

i. Whether PowerSchool received a benefit without proper restitution making it unjust for PowerSchool to retain the benefit without commensurate compensation;

j. Whether PowerSchool violated the Missouri Merchandising Practices Act; and

k. Whether Plaintiff and class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

75. PowerSchool has engaged in a common course of conduct and Class members have been similarly impacted by PowerSchool's failure to maintain reasonable security procedures and practices to protect customers' and users' Private Information.

76. Superiority: A class action is superior to other available methods for the fair and

efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences.

CLASS RELIEF

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class and/or the Missouri Subclass)

77. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

78. PowerSchool required Plaintiff and Class members to provide their Private Information as a condition of using its education technology software and services. PowerSchool collected and stored Plaintiff's and Class members' data for the purposes of providing said services as well as for commercial gain.

79. PowerSchool owed Plaintiff and Class members a duty to exercise reasonable care in protecting their Private Information from unauthorized disclosure or access. PowerSchool acknowledged this duty in its "Global Privacy Statement," "Privacy Principles," (and on various privacy and data related pages on its website) where it promised not to disclose Plaintiff's and Class members' Private Information without their consent.

80. PowerSchool owed a duty of care to Plaintiff and class members to provide security, consistent with industry standards, to ensure that PowerSchool's systems and networks adequately protected its customers' Private Information.

81. PowerSchool's duty to use reasonable care in protecting Private Information arose

as a result of the parties' relationship, as well as common law and federal law, including the FTC Act and PowerSchool's own policies and promises regarding privacy and data security.

82. PowerSchool knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of implementing industry-standard security measures to prevent or detect unauthorized access to user accounts. PowerSchool knew or should have known that it faced an increased threat of customer data theft, as judged by the many data breaches targeted at companies that store Private Information in recent years.

83. PowerSchool breached its duty to Plaintiff and Class members by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to it, including Plaintiff's and class members' Private Information.

84. Plaintiff and class members' Private Information would not have been compromised but for PowerSchool's wrongful and negligent beach of its duties.

85. PowerSchool's failure to take proper security measures to protect the sensitive Private Information of Plaintiff and class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of Private Information by unauthorized third parties. Given the increased threat of customer data theft in education and edtech industries, and extremely high value of Private Information, Plaintiff and Class members are part of a foreseeable, discernible group that was at high risk of having their Private Information misused or disclosed if not adequately protected by PowerSchool.

86. It was also foreseeable that PowerSchool's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiff and Cass members.

87. As a direct and proximate result of PowerSchool's conduct, Plaintiff and Class members have and will suffer damages including: (i) a substantially increased and imminent risk of identity theft—risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) damages for the unconsented disclosure of their Private Information, for which there is a well-established market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Nationwide Class and/or the Missouri Subclass)

88. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

89. PowerSchool's duties arise from Section 5 of the Federal Trae Commission Act ("FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. 15 U.S.C. § 45(a)(1). The FTC publications and orders described above also form part of the basis for PowerSchool's duty in this regard.

90. PowerSchool violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and failing to comply with applicable industry standards. PowerSchool's conduct was unreasonable given the nature and amount of Private Information it

obtained, stored, and disseminated in the regular course of its business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiff and Class members.

91. PowerSchool's violation of Section 5 of the FTC Act constitutes negligence *per se*.

92. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

93. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class members.

94. As a direct and proximate result of PowerSchool's negligence *per se*, Plaintiff and Class members have suffered, and continue to suffer, and will suffer, injuries, damages, and harm as alleged herein.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class and/or the Missouri Subclass)

95. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

96. Plaintiff and Class members provided their Private Information to PowerSchool in the ordinary course of business as a requirement to utilize the education technology software provided by PowerSchool.

97. As part of these transactions, PowerSchool agreed to safeguard and protect the Private Information of Plaintiff and Class members. Implicit in these transactions between PowerSchool and Class members was the obligation that PowerSchool would use the Private Information for approved business purposes only and would not make unauthorized disclosures of

the information or allow unauthorized access to the information.

98. Plaintiff and Class members entered into implied contracts with the reasonable expectation that PowerSchool's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class members believed that PowerSchool would use part of the monies paid to PowerSchool under the implied contracts to fund adequate and reasonable data security practices to protect their Private Information.

99. Plaintiff and Class members would not have provided and entrusted their Private Information to PowerSchool or would have paid less for PowerSchool's services in the absence of the implied contract between them and PowerSchool. The safeguarding of Plaintiff's and Class members' Private Information was critical to realizing the intent of the parties.

100. The nature of PowerSchool's implied promise itself—the subject matter of the contractual provision at issue—was to protect Plaintiff's and Class members' Private Information in order to prevent harm and prevent present and continuing increased risk.

101. PowerSchool breached their implied contract with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' Private Information, which was comprised as a result of the Data Breach.

102. As a direct and proximate result of Defendant's breaches, Plaintiff and Class members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiff and Class members alternatively seek an award of nominal damages.

COUNT IV
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Nationwide Class and/or the Missouri Subclass)

103. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

104. Upon information and belief, acting in the ordinary course of business, PowerSchool entered into contracts with its customers (schools, school districts, and higher education institutions) to provide education technology software and services based on the Private Information it received from its customers, Plaintiffs, and Class members.

105. Upon information and belief, each of those respective contracts contained provisions requiring PowerSchool to protect the Private Information that PowerSchool received in order to provide such education technology services.

106. Upon information and belief, these provisions that require PowerSchool, while acting in the ordinary course of business, to protect the Private Information of Plaintiff and Class members were intentionally included for the direct benefit of Plaintiff and Class members, such that Plaintiff and Class members are intended third-party beneficiaries of these contracts, and therefore entitled to enforce them.

107. PowerSchool breached these contracts while acting in the ordinary course of business by not protecting Plaintiff's and Class members' Private Information, as stated therein.

108. As a direct and proximate result of PowerSchool's breach, Plaintiff and Class members sustained actual losses and damages described in detail herein.

COUNT V
Violation of Missouri Merchandising Practices Act ("MMPA")
Mo. Rev. Stat. § 407.010 *et seq*.
(On Behalf of Plaintiff and the Missouri Subclass)

109. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

110. Plaintiff brings this claim on behalf of herself and the Missouri Subclass who are residents of Missouri.

111. PowerSchool is a "person" as defined by Mo. Rev. Stat. § 407.010(5). Plaintiff and Missouri Subclass members are actual consumers of the products and services offered by

PowerSchool.

112. PowerSchool, operating in Missouri, engaged in deceptive, unfair, and unlawful trade acts or practices in the course of its business, vocation or occupation, in violation of Mo. Rev. Stat. § 407.020, including, but not limited to, the following:

a. Knowingly misrepresenting and fraudulently advertising material facts pertaining to its products and services to the Missouri Subclass by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Missouri Subclass members' Private Information from unauthorized disclosure, release, data breaches, and theft;

b. Knowingly misrepresenting material facts pertaining to its products and services to the Missouri Subclass by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Missouri Subclass members' Private Information;

c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Missouri Subclass members' Private Information (intending to induce others to enter into a transaction);

d. Failing to timely delete Plaintiff and Missouri Subclass members Private Information after it no longer served a reasonable business purpose;

e. Engaging in unlawful practices by failing to maintain the privacy and security of Missouri Subclass members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach; and

f. Engaging in unlawful practices by failing to disclose the Data Breach to Missouri Subclass members in a timely and accurate manner, in violation of Mo. Rev. Stat. § 407.1500.

113. PowerSchool's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of PowerSchool's data security and ability to protect the confidentiality of customers' and users' Private Information.

114. PowerSchool intended to mislead Plaintiff and the other Missouri Subclass members and induce them to rely on its misrepresentations and omissions.

115. Had Plaintiff and the other Missouri Subclass members known that PowerSchool

failed to employ necessary and adequate protection of their Private Information, they would not have utilized PowerSchool's education technology software or services or limited the Private Information they shared with PowerSchool. PowerSchool engaged in the above unfair and deceptive acts or practices in the course of its business.

116. PowerSchool engaged in the above unfair and deceptive acts or practices with malice and/or willfulness.

117. As a direct and proximate result of PowerSchool's unfair and deceptive practices, Missouri Subclass members suffered injuries to legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

118. The practices and acts described above were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the other Missouri Subclass members that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

119. PowerSchool knew or should have known that its computer systems and data security practices were inadequate to safeguard Missouri Subclass members' Private Information and thus, that risk of a data breach or theft was high. PowerSchool's' actions in engaging in the above unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Missouri Subclass.

120. Plaintiff and the other Missouri Subclass members seek relief under Mo. Rev. Stat. §§ 407.010, et seq., including, but not limited to, compensatory damages, punitive damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class and/or the Missouri Subclass)

121. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

122. Plaintiff and Class members have an interest, both equitable and legal, in their Private Information that was conferred upon, collected by, and maintained by PowerSchool and which was stolen in the Data Breach. This information has independent value.

123. PowerSchool benefited by the conferral upon it of Private Information pertaining to Plaintiff and Class members and by its ability to retain, use, and profit from that information. PowerSchool understood and valued this benefit.

124. PowerSchool also understood and appreciated that the Private Information pertaining to Plaintiff and appreciated that the Private Information pertaining to Plaintiff and Class members was private and confidential, and its value depended upon PowerSchool maintaining the privacy and confidentiality of that Private Information.

125. Without PowerSchool's willingness to and commitment to maintain the privacy and confidentiality of the Private Information, Plaintiff and Class members would not have provided and/or entrusted the information to PowerSchool.

126. Because of PowerSchool's use of Plaintiff's and Class members' Private Information, PowerSchool brokered more services than it otherwise would have. PowerSchool was unjustly enriched by profiting from the additional services and programs they were able to broker and in the detriment of Plaintiff and Class members.

127. PowerSchool also benefited through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff's and Class members' Private Information.

128. It is inequitable for PowerSchool to retain these benefits.

129. As a result of PowerSchool's wrongful conduct as alleged in this Complaint (including among other things, its failure to implement reasonable safeguards to ensure the protections of the Private Information belonging to Plaintiff and Class members), PowerSchool has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class members.

130. PowerSchool's unjust enrichment is traceable to and resulted directly and proximately from the conduct alleged herein, including the collection and use of Plaintiff's and Class members' sensitive Private Information, while at the same time failing to implement, monitor, audit, and test its own data security to maintain the security of the information from intrusion and theft by cybercriminals and identity thieves.

131. It is inequitable, unfair, and unjust for PowerSchool to retain these wrongfully obtained benefits. PowerSchool's retention of wrongfully obtained monies violates fundamental principles of justice, equity, and good conscience.

132. The benefit conferred upon, received, and enjoyed by PowerSchool was not conferred gratuitously, and it would be inequitable, unfair, and unjust for PowerSchool to retain the benefit.

133. Plaintiff and Class members have no adequate remedy at law.

134. PowerSchool is therefore liable to Plaintiff and Class members for restitution or disgorgement in the amount of the benefit conferred on PowerSchool as a result of its wrongful conduct, including specifically, the value to PowerSchool of the Private Information that was stolen in the Data Breach; the profits PowerSchool received and is receiving from the use of that information; and the amounts that PowerSchool should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class members' Private Information.

COUNT VII
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Class and/or the Missouri Subclass)

135. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

136. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

137. An actual controversy has arisen in the wake of the Data Breach regarding PowerSchool's present and prospective common law and other duties to reasonably safeguard Private Information and whether PowerSchool is currently maintaining data security measures adequate to protect Plaintiff and Class members from further cyberattacks and data breaches that compromise their Private Information.

138. PowerSchool still possesses Private Information pertaining to Plaintiff and Class members, which means their Private Information remains at risk of further breaches because PowerSchool's data security measures remain inadequate. Plaintiff and Class members continue to suffer injuries as a result of the compromise of their Private Information and remain at an imminent risk that further compromises of their Private Information will occur in the future.

139. Pursuant to the Declaratory Judgment Act, Plaintiff seeks a declaration that: (a) PowerSchool's existing data security measures do not comply with their obligations and duties of cares; and (b) in order to comply with their obligation and duties of care, (1) PowerSchool must have policies and procedures in place to ensure effective monitoring and testing of their security practices and protocols; (2) PowerSchool must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiff's and Class members' Private Information if it is no longer necessary to perform

essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on PowerSchool's systems on a periodic basis, and ordering PowerSchool to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Encrypting Private Information and segmenting Private Information by, among other things, creating firewalls and access controls so that if one area of PowerSchool's systems is compromised, hackers cannot gain access to other portions of its systems;

e. Purging, deleting, and destroying in a reasonable and secure manner Private Information not necessary to perform essential business functions;

f. Conducting regular database scanning and security checks;

g. Conducting regular employee education regarding best security practices;

h. Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

i. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Classes set forth herein, respectfully requests the following relief:

A. That the Court certifies this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representative and Plaintiff's counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent PowerSchool from continuing to engage in unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and Class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court award Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses: and

F. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in the instant action.

Dated: January 28, 2025

/s/ *Norman E. Siegel*
Norman E. Siegel (MO Bar No. 44378)
J. Austin Moore (MO Bar No. 64040)
Brandi S. Spates (MO Bar No. 72144)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel: 816-714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
spates@stuevesiegel.com

Counsel for Plaintiff and the Class